MASTER OF SCIENCE
IN
DEFENSE ANALYSIS

CLANDESTINE COMMUNICATION SYSTEMS
John T. Corley-Major, United States Army
B.S., Virginia Military Institute, 1989
Master of Science in Defense Analysis-December 2001
Advisor: Gordon McCormick, Department of Defense Analysis
Second Reader: George Lober, Department of Defense Analysis

Subversive elements, whether insurgent, terrorist, or criminal, all require a communication system to coordinate and control operations. The development of a clandestine communication system requires special considerations in the development of the nodes and links that are responsible for the transmission of information. A closure analysis of these processes, professionally referred to tradecraft, assists in the planning and development of a communication system to support or counter subversive operations. This thesis analyzes tradecraft as a communication system to identify the constraints and opportunities to which different technologies have proven useful and the strengths and weaknesses of the same.

KEYWORDS: Communication, Clandestine Communication, Subversive, Organizational Communication, Insurgent, Terrorist

COMMAND AND CONTROL OF SPECIALIZED AVIATION ASSETS:
A NEW OPERATIONAL CONCEPT
Reginald F. Davis-Major, United States Air Force
M.S., Embry-Riddle University, 1997
Master of Science in Defense Analysis-December 2001
Advisor: William G. Kemple, Department of Information Sciences
Second Reader: David Tucker, Department of Defense Analysis

Currently, U.S. military forces deploy and employ under the auspices of separate systems. Deployment occurs via the Joint Chiefs of Staff managed process called Joint Operational Planning and Employment System (JOPES). Employment of forces occurs under the direction of a combatant theater commander. In the case of special operations forces, the employment process is managed by a Joint Special Operations Task Force (JSOTF) commander and is known as Time Sensitive Planning. Special operations forces are able to execute jointly planned and rehearsed special operations missions within 96 hours of receiving a warning order. The JOPES deployment system may take days to complete the coordination required to deploy military forces overseas. However, control of those military forces, and therefore mission preparation, does not currently pass to the theater commanders until the forces arrive in theater. Depending on the method of transportation, this deployment window may take as long as a week. Although in some cases, deployments can be accomplished in a matter of days. This is the exception rather than the rule, though. The net effect is that the timeliness of military responses to crises is limited not only by the distance to the frontline, but also by the speed of the current JOPES and mission planning processes. This is true for special operations forces as well as conventional military forces. This thesis will offer a new operational concept for the deployment, employment, and command and control of specialized air power.

KEYWORDS: Special Operations, SOF, Command and Control, Concept of Operations, Aviation

ASYMMETRIC WARFARE AND THE WILL TO WIN

Cary A. Herrera-Major, United States Air Force
B.S., United States Air Force Academy, 1987
M.S., Troy State University, 1996
Master of Science in Defense Analysis-December 2001
and
Matthew D. Quinn-Major, United States Army
B.S., Rochester Institute of Technology, 1990
Master of Science in Defense Analysis-December 2001
Advisor: Anna Simons, Department of Defense Analysis
Second Reader: George Lober, Department of Defense Analysis

This thesis explores the *will to win* in asymmetric war. Asymmetric war, in which one side has an overwhelming advantage over its opponent, will likely be the war of the future for the United States in the post-Cold War uni-polar world. To win an asymmetric war, the individual and then the masses must be motivated to fight and, ultimately, the *will to win* must be cultivated and sustained for victory. Religion is a highly effective motivator for both the individual and the masses. This motivation, when properly directed, can provide the *will to win* in the face of overwhelming odds.

This thesis focuses on religion as the primary motivator in an asymmetric war. Religion is a strong motivator for the individual because of four factors: appropriateness, identity, rationality, and religion's strength as an internally consistent logic. With a highly motivated individual, an organization gains specific advantages by focusing on the religious aspects of the conflict. These advantages are: commitment, legitimacy, membership, and longevity. These are the measurable elements that create a strong *will to win*.

Three case studies – Iran and Iraq, Hezbollah and Israel, and the Islamic Salvation Front (FIS) and Algeria - are explored as examples of contemporary asymmetric conflict. These case studies are used to examine the asymmetries between the countries in conflict and test the validity of our theory about the significance of the will to win.

KEYWORDS: Asymmetric Warfare, Motivation, Religion, Iran, Iraq, Hezbollah, Israel, Islamic Salvation Front, Algeria

ON DECEIVING TERRORISTS

Benjamin I. Higginbotham-Captain, United States Army
B.S., Texas A&I University, 1990
Master of Science in Defense Analysis-December 2001
Advisor: John Arquilla, Department of Defense Analysis
Second Reader: Wayne Hughes, Graduate School of Operations and Information Sciences

This thesis addresses the use of deception as one means available to states for dealing with terrorists. It begins by exploring the body of theoretical literature to establish the foundation necessary for a thorough discussion of deception. Next, the thesis examines the reasons for state use of deception in interstate conflict. From this list, three potential uses of deception against terrorists are suggested. Specifically, the thesis proposes that states use deception to create and exploit organizational inefficiencies and weaknesses in terrorist organizations, facilitate counter-terrorist operations, and conceal counter-terrorist capabilities and intentions. Subsequently, the cases presented herein reveal that states have in fact successfully used deception in the past with all three purposes in mind. Finally, this thesis also explores the often-overlooked subject of risks and costs, demonstrating that the use of deception is almost never without expense. Even when deception succeeds, its use inevitably incurs costs and opens the door to certain risks. Moreover, the study shows that deception—while both legal and ethical in the larger sense—might be illegal or unethical in certain applications. In the end, this thesis shows that deception is, indeed, a valuable tool against terrorists.

KEYWORDS: Deception, Special Operations, Terrorism, Counter-Terrorism, Intelligence, Counter-Intelligence, Information Warfare

AN ANALYSIS OF THE NAVAL SPECIAL WARFARE TWENTY-ONE TRANSFORMATION

Louis M. McCray-Lieutenant, United States Navy
B.A., University of San Diego, 1996
Master of Science in Defense Analysis-March 2002
and
Steven K. Renly-Lieutenant Commander, United States Navy
B.A., National University, 1987
Master of Science in Defense Analysis-December 2001
Advisor: Anna Simons, Department of Defense Analysis
Second Reader: Gordon H. McCormick, Department of Defense Analysis

Can we ever *truly* understand what motivates us to act in particular ways? Can we draw inferences from our understanding of the actions of one to explain the behaviors of many? Can we ever hope to develop broad theories that make human behavior comprehensible? This thesis is inclined to say no. However, this "no" is only a tentative answer. Throughout this thesis we will discuss, observe, and analyze these questions of human behavior in the context of organizational theory: a discipline that is essentially a study of how humans act when they group themselves into bureaucratic organizations. In this thesis, we will use Naval Special Warfare and its NSW-21 transformation effort as an example of how an organization changes, *even when* that change seems to go against the grain of popular wisdom.

We have approached this thesis from the perspective of a curious workman who has just opened the back of a clock to see what makes the timepiece tick. As we analyze what makes Naval Special Warfare tick, we will tell the story of the NSW-21 transformation. In this work, we seek to satisfy three objectives: 1) to provide a broad understanding of NSW-21 and its implications, 2) to explain why NSW-21 was a smart move for the Naval Special Warfare community, and 3) to use Naval Special Warfare's recent transformation endeavors as a means to understand how and why groups must organize, reorganize, and transform themselves in order to meet the challenges of the 21st century. Essentially, this thesis can be boiled down to one simple question: "Why does the NSW-21 transformation make sense for Naval Special Warfare?"

KEYWORDS: Organizational Studies, Behavioral Research, Organizational Transformation in the Information Age

UNCONVENTIONAL ASSISTED RECOVERY (UAR): HISTORICAL CASE STUDY ANALYSIS AND QUANTITATIVE FEASIBILITY ASSESSMENT

Eric A. Patterson-Captain, United States Army
B.S., United States Military Academy, 1991
Master of Science in Defense Analysis-December 2001
Advisor: Gordon McCormick, Department of Defense Analysis
Second Reader: Frank Giordano, Department of Mathematics

During the Gulf War, 34 Coalition pilots were shot down, yet only six were recovered by conventional CSAR. Consequently, SOF planners began to consider the impact of integrated air defenses upon personnel recovery and to consider a more proactive method of recovery. While serving as a member of the SOCCENT Unconventional Warfare Working Group and as the lead planner for the first UAR training program and exercise for 3rd Special Forces Group, I observed that there was little consideration of similar historical operations and that operators were skeptical of UAR. The purpose of this thesis is to assist the special operations community with the development of doctrine for UAR and to offer SOF commanders a feasibility assessment tool. This purpose was achieved by: (1) Developing a historical perspective of similar missions through case study analysis to determine, via controlled comparison, the key independent variables that determine the success of ground-based SOF recovery operations, and by (2) Conducting quantitative modeling of UAR to determine, through a range of numerically based conditions, a range of feasibility and doctrinal implications for UAR.

KEYWORDS: Unconventional Assisted Recovery, UAR, Non-conventional Assisted Recovery, NAR, Personnel Recovery, Evasion, Rescue, Unconventional Warfare, Special Operations, Special Forces

FUTURE WARFARE AND THE SPECIAL OPERATIONS COMMAND BUDGET
Gerard F. Quinlan-Lieutenant Commander, United State Navy
B.S., Utica College of Syracuse University, 1988
Master of Science in Defense Analysis-December 2001
Master of Science in Management-December 2001
Advisors: Gordon McCormick, Department of Defense Analysis
Jerry McCaffrey, Graduate School of Business and Public Policy

This thesis will first suggest that future military intervention for the United States will primarily revolve around low intensity conflict, guerrilla warfare and other irregular military involvement. The paper will then segue into describing how the Special Operations Command (SOCOM) is the force of choice in order to meet many of the upcoming challenges that the United States will face if the above assertion holds true.

Having established the link between future military intervention and Special Operations Forces (SOF), the study will then analyze prior years SOCOM budgets, unclassified strategic guidance as well as evidence of the demand for SOF in an effort to answer two questions.

The first question asks whether or not SOCOM's budget would be able to support an increase in employment of SOF at an acceptable readiness level. The second question asks if SOCOM requires more funding to remain capable and effective in the future. The answers to these questions are the thrust of this study.

KEYWORDS: Special Operations Command, Special Operations Command Budget, Special Operations Command Readiness

CYBERTERROR: WAITING FOR THE SKY TO FALL (U)
John W. Wheeler-Major, United States Army
B.S., United States Military Academy, 1989
Master of Science in Defense Analysis-December 2001
and
Patrick M. Foster-Lieutenant, United States Navy
B.S., Southern Illinois University, 1993
Master of Science in Defense Analysis-December 2001
and
Tyler K. Moore-Captain, United States Air Force
B.S., United States Air Force Academy, 1993
Master of Science in Defense Analysis-December 2001
Advisor: John Arquilla, Department of Defense Analysis
Second Reader: David Tucker, Department of Defense Analysis

Our thesis addresses the issue of cyberterrorism. We initially define cyberterror and other technical terms. We then explore the varying levels of skill required for an organization to engage in cyberterror and the milestones for achieving these levels. The case studies in the paper highlight terrorist organizations and hacktivist groups with the greatest capabilities for engaging in cyberterrorism. We specifically consider Aleph (formerly Aum Shinrykyo), Al Qaeda, mOs, Serbian Black Hand, and the Chinese Honker's Union (HUC). The examination of the capabilities and goals of these organizations indicates a viable threat to the United States exists from these groups. The second section of our thesis addresses the defensive posture of the United States as it currently exists. We begin with a review of the organizations involved in our national cyber defense strategy, and their abilities to provide information assurance and computer network defense. We then evaluate the defense in depth model for cyber defense and suggest some methods for improving the current model. We conclude with a discussion of potential methods for deterring cyberterrorist attacks against the United States, concluding with an assessment on the future of cyberterrorism.

KEYWORDS: Cyberterrorism, Aleph, Al Qaeda, Muslim Online Syndicate, Serbian Black Hand, Honkers Union of China, Critical Infrastructure Protection, Information Assurance, Encryption, Deterrence